Vot.Ar: una mala elección

Francisco Amato, Iván A. Barrera Oro, Enrique Chaparro, Sergio Demian Lerner, Alfredo Ortega, Juliano Rizzo, Fernando Russ, Javier Smaldone, Nicolas Waisman

2a versión, julio 2015
CABA, Argentina

@famato
@hackancuba
–
@SDLerner
@ortegaalfredo
@julianor
–
@mis2centavos
@nicowaisman

Abstracto— Con el anuncio del Tribunal Superior de Justicia de la Ciudad de Buenos Aires de la implementación de un sistema de votación electrónico para la Ciudad, basado en boletas con chip RFID, decidimos investigar el asunto a sabiendas de casos de fracaso internacional por ser los sistemas como éste inseguros y para ciertos países, inconstitucional. El objetivo del presente informe es verificar si este sistema es también inseguro y/o vulnerable, poner en evidencia los riesgos que implicase su empleo y contrastarlos con el empleo de la boleta única de papel.

I. INTRODUCCIÓN

El 8 de junio de 2015 el Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires aprueba el sistema de Boleta Electrónica mediante la resolución 127/15 [1], donde reza: "Por Resolución n° 126, el Tribunal aprobó "…para la elección del 5 de julio y eventual segunda vuelta del 19 de julio, la aplicación de tecnologías electrónicas en la etapa de emisión del voto, escrutinio de sufragios y transmisión y totalización de resultados electorales provisorios, con el sistema de la empresa contratista del GCBA, auditado por la Universidad de Buenos Aires, en los términos del art. 25, del anexo II, ley nº 4894" y por artículo 2 se aprobaron las pantallas con las listas de todas las agrupaciones políticas, de acuerdo con la secuencia aprobada por la Acordada Electoral nº 17/15".

Este sistema, llamado BUE y desarrollado por la empresa Grupo MSA bajo la denominación “vot.ar” consta de dos partes principales: máquina de emisión de voto y boleta única electrónica (BUE). La primera se trata de una computadora portátil embebida en una caja que posee una pantalla táctil y un lector/escritor RFID e impresor de boletas. La segunda consta de una lámina de papel grueso con la propiedad de poder ser impreso térmicamente y conteniendo un chip con tecnología RFID.

El usuario inserta una boleta en blanco en la ranura correspondiente de la máquina y selecciona en la pantalla la lista o candidatos deseados. Al finalizar, la máquina imprimirá lo seleccionado sobre la boleta (impresión térmica) y asimismo escribirá electrónicamente en el chip RFID estos mismos datos.

El presente informe demostrará que el sistema es / puede ser **vulnerable** en los siguientes puntos:

- el chip de la BUE puede ser leído por un tercero,
- el chip de la BUE puede ser escrito nuevamente por un tercero [2],
- la impresión térmica posee una vida media corta, anulando auditorías o revisiones futuras sobre un proceso electoral [3],
- el hardware de la máquina puede ser accedido por terceros de manera local, pudiendo causar:
    - impedir su normal funcionamiento,
    - anular, modificar o leer votos, violando el Art. 37 de la Constitución Nacional “El sufragio es universal, igual, secreto y obligatorio.” [4],
    - conectar un aparato de transmisión remoto de datos.

Hemos tenido acceso a las máquinas situadas en distintos puntos de la ciudad, y a máquinas proveídas por MSA durante una auditoría privada que no cabe en el marco de la presente y que sin embargo fue muy limitada. El hardware es fundamental, dado que los equipos utilizados en las elecciones no han sido certificados en ningún punto del proceso, situación que pone en jaque la seguridad del sistema. Consideramos que esta falla es del tipo crítica.

II. SOBRE VOT.AR

Vot.Ar es una creación del Grupo MSA con el objeto de implementar un sistema de Boleta Única Electrónica (BUE).

En su página web [5] se autodefine como:

1. Secreto
2. Seguro
3. Transparente
4. Igualitario

Respecto de estas pautas y con los elementos que serán expuestos en el presente, demostraremos que:

1. El voto puede ser leído por terceros, por tanto no es secreto;
2. El sistema es vulnerable, por tanto no es seguro;
3. El sistema posee hardware cerrado y código cerrado, no libre [6] y [7], por lo tanto no es transparente;
4. Aún si los electores, fiscales y demás intervinientes en el acto electoral son capacitados para el uso del sistema, proceso que en principio se estaría llevando a cabo por el TSJ CABA [8], y el Gobierno de la Ciudad junto al Grupo MSA en Centros de Consulta [9] y aún teniendo en cuenta a las personas con discapacidades visuales o auditivas, es nuestra consideración, puesto que no es posible comprender la totalidad del funcionamiento del sistema sin poseer conocimientos técnicos avanzados, que muy difícil resulta afirmar que el mismo sea igualitario.

Debemos destacar que la empresa no ha facilitado la realización de este informe, así como sucedió con el informe del Departamento de Informática del ITBA que ampliaremos en el punto IV. A, violando de esta manera el Inciso 3.4.1, ítem 2, del pliego de la licitación pública 2-SIGAF-2015 de la CABA: “El contratista deberá proveer al conocimiento y acceso, a los programas fuentes, funcionamiento de las máquinas de votación, sus características y programas (tanto hardware como software)“ y el Artículo 24, inciso “b” del anexo 2 de la ley 4894 de la CABA [10]: “Tanto la solución tecnológica, como sus componentes de hardware y software debe ser abierta e íntegramente auditable antes, durante y posteriormente a su uso”.

III. CÓMO SE VOTA

Al momento de la elección, se dispondrán máquinas y BUE para cada lugar destinado a tal fin. El Presidente de Mesa abrirá la mesa habilitando la máquina mediante una tarjeta especial (tarjeta azul), quedando así lista para operar. Luego los electores podrán realizar el sufragio. Nos hemos presentado en un punto de consulta y hemos filmado un video demostrativo del proceso de inicialización del sistema y sufragio [11].

Finalizado el proceso, el Presidente introduce la boleta de inicialización donde se imprimirá la fecha y hora (timestamp), su nombre y los nombres de hasta tres Fiscales de Mesa, a los efectos de registrar la apertura de mesa y que conservará para sí como comprobante.

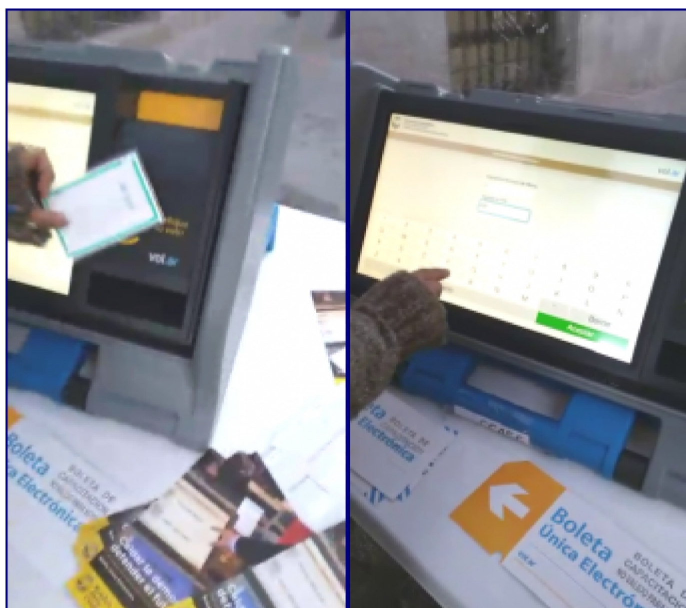
A. Inicialización del sistema

El Presidente de Mesa recibe una tarjeta con chip RFID especial, un PIN, un DVD entregado en sobre lacrado y dos “boleta de inicialización” (boleta azul). Dicho DVD contiene el software de votación.

Se introduce el DVD en la lectora de la máquina y se enciende la misma. Cuando el software haya iniciado, solicitará al usuario calibrar la pantalla presionando en las 4 esquinas de la misma y luego en el centro. Estos pasos serán indicados por unos puntos y cruces que aparecerán en la pantalla.

B. Apertura de mesa

Una vez calibrada la pantalla, el Presidente de Mesa abrirá la mesa identificándose con la tarjeta, introduciendo el número de mesa y su PIN, como se muestra en las Fig. 1 y 2.



Luego, la máquina se encontrará lista para ser operada por los votantes y realizar el sufragio.

C. Proceso de sufragio

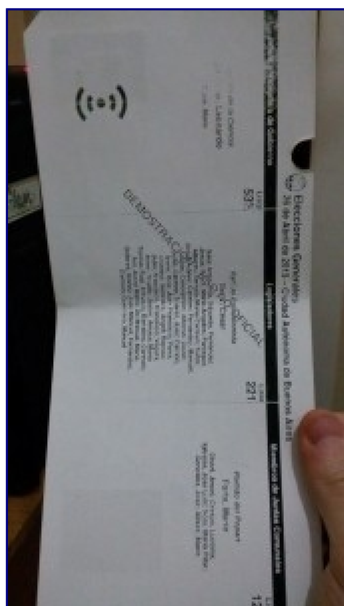
El votante se presenta a la mesa correspondiente y se identifica mediante DNI. Elige aleatoriamente una BUE y el Presidente corta un troquel de la misma y lo retiene

junto al DNI. Luego el votante toma la BUE y se dirige hacia la máquina. Introduce la boleta en la ranura, como se aprecia en la Fig. 3 y elige de la pantalla el/los candidato/s o lista/s de candidato/s (ver Fig. 4).



Al finalizar la selección, se procede a imprimir la BUE:

- Se imprime en la boleta, mediante impresión térmica, los candidatos elegidos (detalle en Fig. 5).
- Se almacena digitalmente esta misma información en el chip RFID (ver punto IV. B para mayor abundamiento).



El votante toma la boleta impresa, se dobla hasta la línea indicada y se dirige a la Mesa; recorta un segundo troquel de la misma, que se entrega al Presidente para constatar que la boleta no ha sido reemplazada por otra y se introduce la misma dentro de la urna.

Finalmente, el Presidente le devuelve el DNI al votante junto con un comprobante de voto y concluye el proceso de sufragio.

D. Cierre de mesa

Al término del horario electoral, el Presidente debe realizar el cierre de la mesa, proceso idéntico al de Apertura de mesa descrito en el punto III. B. Conservará esta segunda boleta azul como comprobante de cierre de mesa.

E. Escrutinio de votos

Cerrada la mesa se inicia el proceso de escrutinio de los votos. Los técnicos conectan la máquina a la red, el Presidente inicializa el proceso y se leen los votos uno a uno aproximando la BUE al lector RFID. Luego se cuentan las boletas y se verifica que el número de votos registrados por el sistema sea igual a la cantidad de boletas; esto es necesario en caso de que alguna boleta no haya sido leída correctamente [12].

Si el resultado es correcto, se sellan las boletas en una bolsa y se imprime un certificado de escrutinio que contiene las cantidades registradas y, que es simplemente una boleta similar a la boleta azul y de igual efecto comprobatorio.

Finalmente se emite el recuento al servidor central.

IV. ANÁLISIS DETALLADO DE SISTEMA

Hemos realizado esta investigación haciendo uso de las máquinas de capacitación que se encuentran distribuidas por la ciudad [9].

A. Software vot.ar

El software empleado se trata de un programa escrito mayormente en lenguaje Python y que funciona sobre un sistema operativo Ubuntu. Los detalles sobre el sistema operativo se encuentran en el Apéndice A.

La empresa proveerá al TSJ de la imagen de DVD con el software necesario a los efectos de que éste realice grabaciones de discos DVD y los entregue en sobre lacrado el día electoral. No contamos con mayor detalle de este proceso.

La imagen en cuestión es arrancable (booteable), esto es, la PC puede iniciar el sistema operativo desde el mismo. Con el objeto de validar los DVD, la empresa entrega asimismo los hashes de los archivos contenidos, que se trataban en principio de hashes MD5 y luego fueron reemplazados por SHA512, según indica el Sr. Fisanotti, empleado de MSA [13]. En nuestras pruebas, si bien se encontró el

archivo sha512sum.txt, el mismo no es usado en ningún momento por el software, sino que se usa el archivo conteniendo hashes MD5 md5sum.txt [14]. No existe diferencia real respecto de la validación de archivos, dado que sin importar el algoritmo empleado, este archivo puede ser generado por cualquier persona. No está firmado digitalmente, dando cuenta de un grave error de apreciación de seguridad.

El software desarrollado por MSA para realizar el proceso de sufragio ha sido auditado por el Departamento de Computación de la Facultad de Ciencias Exactas y Naturales de la Universidad de Buenos Aires (FCEyN-UBA) [15], encontrando algunos errores y problemas catalogados como menores, diciendo cumplir los requisitos mínimos para ser empleado en un acto eleccionario, diagramados en el Anexo II de la Ley 4894/13 [10] y [16].

Del informe pueden destacarse lo siguiente:

> “Los defectos en la documentación representan un punto débil a observar en el software que dificulta no sólo la auditabilidad del mismo, sino también el mantenimiento y la evolución” [17].

> “[…] es crucial para el correcto funcionamiento [del sistema] en forma global que las autoridades de mesa, delegados judiciales y demás responsables de los comicios sigan los procedimientos aprobados por el Tribunal (Acordada 17/2015, Anexo II) […]” [18].

El Anexo I detalla puntos débiles del software como funciones no recomendadas y demás. Se indica que el software es válido para ser empleado en un acto eleccionario debido a que “la voluntad de los electores se puede verificar en forma completamente manual” [19], esto es, aún alterando el contenido del chip RFID de la BUE, se puede verificar manualmente observando los valores impresos.

Si bien esto es cierto, destacamos el hecho que este sistema, al ser vulnerable como se demuestra en los puntos IV. B, C y D, requiere de un conteo manual y además “la única forma de asegurar la confiabilidad de los comicios con este sistema es, al igual que en el sistema tradicional de boletas preimpresas con sobres, que las autoridades de los comicios sepan los procedimientos que deben seguir y lo hagan.” [20], que nos conduce a preguntarnos cuál es el objetivo de emplear este sistema si no implican ventajas respecto de la boleta única de papel.

Asimismo, siendo que la misma máquina que se emplea para emitir el voto se usa para verificarlo, un usuario malintencionado podría adulterar lo indicado por dicha máquina tal de mostrar lo que el votante desea ver, no siendo esta acción una

medida de seguridad suficiente. Destacamos que aún existiendo el voto impreso, la máquina solo puede contar los votos mediante el chip por lo que si el contenido del chip ha sido adulterado, ese valor será contado válido y no lo impreso. Incluso durante el escrutinio manual posterior, salvo orden en contrario, no contabilizan nuevamente todos los votos, sino aquellos que presentaron algún inconveniente como los “no leído por razones técnicas”. Esto sucedió así en las elecciones del 5 de julio. Al no considerarse el valor impreso – verificación última -, el sistema queda expuesto a la acción de un usuario malintencionado atacando a través del chip RFID (ver puntos IV. C. 3 y Apéndice B).

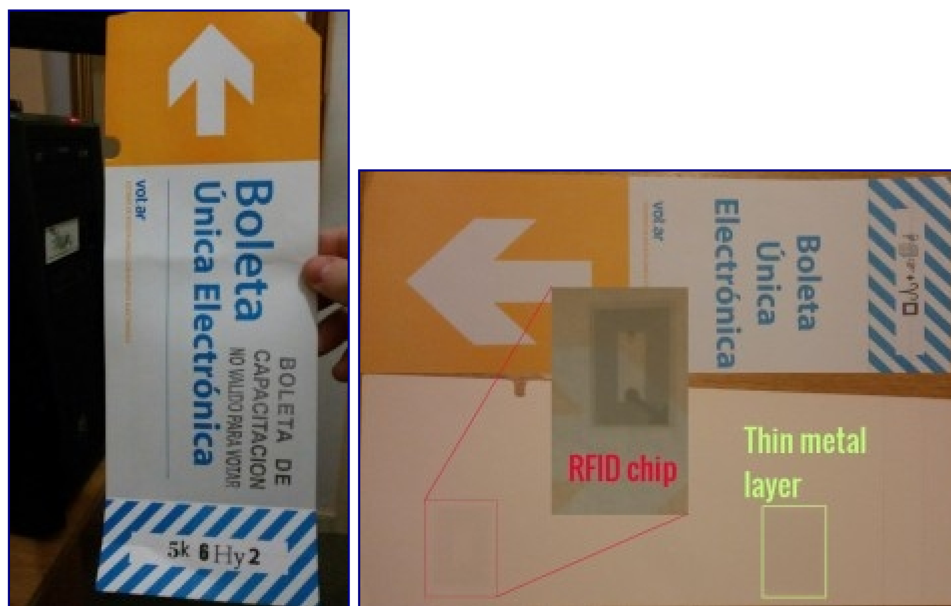
La Defensoría del Pueblo de la Ciudad encargó una auditoría al Departamento de Informática del ITBA [21], fechado 9 de junio, del que se destaca: “se nos informó que el hardware presentado y la versión software del sistema auditado no son necesariamente los que se utilizarán en la elección de la Ciudad de Buenos Aires el próximo mes de Julio” [22]. Luego menciona las limitaciones de la auditoría y finalmente concluye entregando 10 recomendaciones como “se debe auditar el sistema completo (hardware, software, comunicación) definitivo a instalar en las máquinas de votación, con anterioridad a los comicios. Una vez que el TSJ (o quien el tribunal disponga) haya auditado el hardware y el DVD con la versión definitiva, la empresa ya no debería introducir ningún cambio en el sistema, sin volver a ser auditado en su totalidad” [23] y “al momento del escrutinio es recomendable cotejar el dato impreso con el digital, con lo cual se puede aportar verificación al sistema electrónico. Aunque en la Acordada 17/2015 se indica que cuando una BUE no puede ser leída por la máquina se considera como ‘voto no leído por motivos técnicos’, falta discriminar el procedimiento a seguir si el voto impreso no coincidiera con el leído electrónicamente” [24], de las cuales ninguna del total ha sido implementada en las pasadas elecciones.

Del análisis del código fuente resulta llamativa la falta de documentación o que la misma resulta incorrecta, el no uso de pruebas unitarias, la dificultad de mantener el código dada la escasa pulcritud que presenta; todos los elementos que hacen a las buenas prácticas del arte de la informática han sido omitidos, como destacan también las mencionadas auditorías. Estas malas prácticas tienden a facilitar la existencia de bugs y dificulta las auditorías y el mantenimiento del código.

B. Tarjeta BUE

La tarjeta o boleta única electrónica (BUE) consiste en una lámina gruesa de papel, de forma rectangular y de tamaño aproximado de 30 cm por 11 cm, conteniendo un

chip RFID del fabricante NXP modelo ICODE SLI SL2 ICS20 [25] para las boletas de capacitación y SLIX SL2S2002 [70] para las de votación e impresa al dorso con una flecha que indica el sentido de inserción en la máquina, el título de la boleta y los troqueles, como se aprecia en la Fig. 6 y 16. La BUE para votar es de color amarillo.



El reverso se encuentra inicialmente en blanco, indicándose con un símbolo de antena la ubicación del chip RFID (ver Fig. 5).

Se ha realizado la lectura del chip en cuestión empleando un teléfono móvil Samsung Galaxy S3 Neo (GT-I9301I) - pudiendo repetirse ésto con cualquier lector RFID compatible con ISO 15693 - obteniendo la siguiente información mediante el software NFC TagInfo scan by NXP (versión 3.0) para Android:

```
-- INFO ------------------------------
 # IC manufacturer: NXP Semiconductors
 # IC type: ICODE SLI (SL2ICS20)
-- NDEF ------------------------------
 # NFC data set storage not present: Maximum NDEF storage size after format: 106 bytes
-- EXTRA ------------------------------
 # Memory size: 112 bytes
 * 28 blocks, with 4 bytes per block
 # IC detailed information:
 Supported read commands:
 * Single Block Read
 * Multiple Block Read
 * Inventory Read
 * Fast Inventory Read
 * Get Multiple Block Security Status
 * Get System Information
 AFI supported
 DSFID supported
 IC reference value: 0x01
```

```
 Capacitance: 23.5 pF
-- TECH ------------------------------
 # Technologies supported:
 ISO/IEC 15693-3 compatible
 ISO/IEC 15693-2 compatible
 # Android technology information:
 Tag description:
 * TAG: Tech
 [android.nfc.tech.NfcV, android.nfc.tech.NdefFormatable]
 android.nfc.tech.NdefFormatable
 android.nfc.tech.NfcV
 * Maximum transceive length: 253 bytes
 MIFARE Classic support present in Android
 # Detailed protocol information:
 ID: E0:04:01:00:25:88:35:F1
 AFI: 0x00
 DSFID: 0x00
 # Memory content:
 [00] . 1C 01 00 1B |....|
 [01] . 78 AF 3A 12 |x.:.|
 [02] . 30 34 43 41 |04CA|
 [03] . 42 41 20 20 |BA  |
 [04] . 20 43 4F 4D | COM|
 [05] . 20 34 39 4A | 49J|
 [06] . 45 46 20 37 |EF 7|
 [07] . 33 4C 45 47 |3LEG|
 [08] . 20 38 33 00 | 83.|
 [09] . 00 00 00 00 |....|
 [0A] . 00 00 00 00 |....|
 [0B] . 00 00 00 00 |....|
 [0C] . 00 00 00 00 |....|
 [0D] . 00 00 00 00 |....|
 [0E] . 00 00 00 00 |....|
 [0F] . 00 00 00 00 |....|
 [10] . 00 00 00 00 |....|
 [11] . 00 00 00 00 |....|
 [12] . 00 00 00 00 |....|
 [13] . 00 00 00 00 |....|
 [14] . 00 00 00 00 |....|
 [15] . 00 00 00 00 |....|
 [16] . 00 00 00 00 |....|
 [17] . 00 00 00 00 |....|
 [18] . 00 00 00 00 |....|
 [19] . 00 00 00 00 |....|
 [1A] . 00 00 00 00 |....|
 [1B] . 57 5F 4F 4B |W_OK|
 x:locked, .:unlocked
-------------------------------------
```

Esta tarjeta ha sido obtenida de un Centro de Consulta.

El parámetro indicado como ID representa un identificador único e irrepetible del

chip, que asimismo no puede modificarse. Este parámetro reside incrustado en el chip y es generado aleatoriamente por el fabricante.

El detalle de Memory content muestra a izquierda el número de bloque de memoria, luego el contenido de dicho bloque y a derecha la representación ASCII (legible por humanos) de los datos. Se destacan los valores de Miembros de Juntas COMunales, JEFe y Vicejefe de Gobierno y LEGisladores.

Todos los valores presentados, a excepción del ID, pueden ser alterados fácilmente empleando cualquier software afín, como ser por ejemplo NfcV-Reader by STMicroelectronics para Android.

Este tipo de chip RFID puede bloquearse contra escritura según indica el fabricante [26], y se ha determinado que sí es implementado por el sistema Vot.Ar. En el caso de realizarse escritura manual sobre el chip (esto es, sin emplear la máquina de votar), la activación o no del bloqueo de escritura corre por cuenta del usuario. Una vez bloqueada la escritura, no es posible desbloquearla sin implicar la destrucción del mismo, según indica el fabricante.

Sin embargo, la lectura no puede bloquearse en lo que al chip respecta. A este fin, han incorporado en la tarjeta una fina lámina metálica que, al doblar la tarjeta hasta la línea indicada, impide la lectura de la misma sí y solo sí la distancia entre las caras, en particular entre el chip y la lámina, es inferior a aproximadamente 8mm, medición obtenida en pruebas con el hardware antes mencionado, por lo que ésta puede variar para otro hardware lector. No consideramos que este mecanismo sea suficiente, en especial siendo que luego de introducir la boleta en la urna, la misma tenderá a abrirse, permitiendo así su lectura remota.

B. 1. Estructura de datos

El chip en cuestión permite almacenar hasta 112 bytes. Dentro de la memoria, se designan los bytes de la siguiente manera:

K1 T2 T1 L1 C4 C3 C2 C1 D1...Dn W1 W2 W3 W4

El primer byte, K1, corresponde a un Token. Solo hemos encontrado como válido el valor 0x1C.

El segundo y tercer byte, T2 T1, corresponden al tipo de boleta, almacenado como little-endian, y los valores posibles son:

- 0x0000: Tag Vacío
- 0x0001: Tag Voto

- 0x0002: Tag de técnico
- 0x0003: Tag de Presidente de Mesa
- 0x0004: Tag especial para escrutinio
- 0x0005: Tag especial para apertura
- 0x0006: Tag demostración
- 0x0007: Tag virgen
- 0x007F: Tag especial de transmisión
- 0x0080: Tag addendum
- 0xFFFF: Tag desconocido

En la boleta de ejemplo se observa 0x0100.

El cuarto byte, L1, indica la longitud en bytes que ocuparán los datos (D1…Dn). En la boleta de ejemplo: 0x1B, que indica 27 bytes de datos.

Los bytes quinto a octavo, C4 C3 C2 C1, corresponden al CRC32 de los datos, también almacenado como little-endian. En la boleta de ejemplo: 0x123AAF78.

Desde el noveno byte hasta la cantidad indicada por L se encuentran los datos, D, codificados en ASCII. En la boleta de ejemplo: "04CABA COM 49JEF 73LEG 83". El primer texto 04CABA corresponde a la ubicación de la máquina, es decir, el número de mesa en la que se está votando. Normalmente se encuentra un texto como "06CABA.2" donde 06 es la longitud, escrita como números ASCII, de la ubicación en sí (CABA.2), luego CABA corresponde a la ciudad y separado por un "." se encuentra en número de mesa. Otro ejemplo: "09CABA.2188"

Finalmente, el último bloque de 4 bytes de memoria, W1 W2 W3 W4, corresponden a una prueba de escritura aparentemente realizada por la empresa y no es empleada por el sistema en ningún momento. Suele contener en ASCII y big-endian el texto "W_OK".

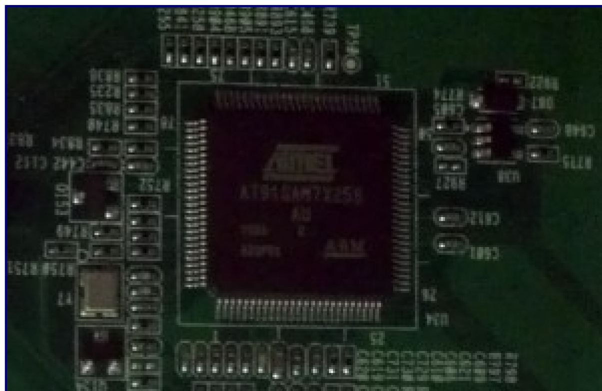
Las boletas especiales, como de Presidente de Mesa o Técnico solo poseen 3 bytes: el token y el tipo de tarjeta. Pueden fabricarse con facilidad mediante un teléfono con NFC y cualquier aplicación que escriba en el chip los datos indicados, dado que no cuentan con ningún tipo de verificación.

C. Hardware vot.ar

La máquina consta de 2 partes principales o subsistemas: pantalla (PC all-in-one) a la izquierda y lector/grabador RFID + impresora térmica a la derecha. En la Fig. 7 se aprecia la misma.



No hemos sido proveídos por MSA de acceso al hardware por tiempo suficiente para realizar más pruebas en profundidad, o analizar los mecanismos internos de éste en su totalidad. Sin embargo destacamos que el sistema cuenta con un procesador central Intel Atom o Celeron y un microcontrolador ARM Atmel AT91SAM7X256 [27] que se aprecia en la Fig. 8. El mismo se encarga de manejar el subsistema de impresión de boleta y lector/escritor RFID.



C. 1. El subsistema PC all-in-one

En la parte superior de la pantalla existe una tapa que da acceso a los puertos de la PC – ver Fig. 9 -, de los que se destacan los puertos USB. Esto implica una enorme vulnerabilidad en caso de no restringirse el acceso a dicha sección, dado que un atacante puede conectar el dispositivo que desee y tomar control del sistema. Se ha probado conectar un teclado inalámbrico Genius SlimStar 8000 GK-100012/K y obtenido mediante el mismo el control del sistema: si bien las terminales virtuales (TTY) se encuentran deshabilitadas a excepción de la primera, que ejecuta el sistema vot.ar (programa en Python), resulta trivial anularlo p.e. reiniciando el sistema y cambiando la orden de arranque del mismo, obteniendo acceso total como administrador (root).



Si esta vulnerabilidad no es cubierta en las máquinas dispuestas en fecha electoral, cabe destacar que sistema pierde por completo su fiabilidad.

Son vectores de ataque posibles teniendo acceso físico:

- cargar un virus o script desde una unidad USB, como ser BadUSB [28] (el ataque BadUSB no puede impedirse de ninguna manera, es inherente a los puertos USB),
- registrar votos con fecha y hora,
- modificar los votos emitidos (no solo el contenido del chip sino también la impresión, que podría pasar desapercibido si el votante no verifica en otra máquina no afectada),
- transmitir remotamente toda la información procesada, anular por completo el funcionamiento de la máquina (denegación de servicio), p.e. con una bomba lógica (bash fork-bomb u otras),
- reprogramar el susbsitema gestionado por el ARM.

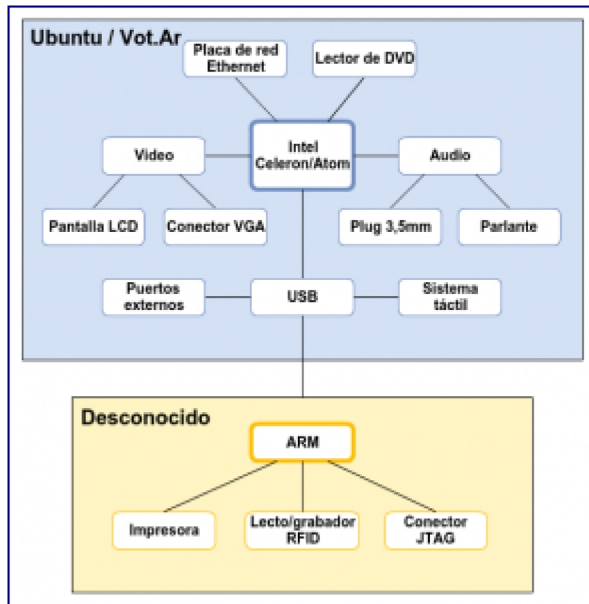
C. 2. El subsistema de impresión y RFID

El microcontrolador ARM Atmel AT91SAM7X256 se encarga de gestionar el lecto/grabador RFID ISO/IEC 15693 y la impresora térmica. Es accesible en el subsistema PC como un dispositivo serial, nomenclado “ttyACM0" en Linux, como puede apreciarse en el módulo armve del software Vot.Ar [29].

No hemos logrado acceder al firmware así como tampoco a su código fuente, representando otro punto oscuro del sistema violando el Art. 24, inc. b, Anexo II de la Ley 4894 de la CABA como indicáramos en el punto II.

El diagrama de la Fig. 10 muestra una representación macroscópica del sistema, de lo que hacemos mención puesto que, como todo microcontrolador, éste cuenta con memoria EEPROM integrada de 256KB [30] que le permite almacenar todo tipo de información, como ser p.e. el voto y una marca de tiempo (timestamp), y al actuar con software desconocido, resulta imposible determinar qué acciones está llevando

a cabo durante el proceso electoral, situación que consideramos de gravedad crítica. Es posible también reprogramarlo en tiempo de ejecución mediante la interfaz JTAG.



En los equipos analizados, encontramos acceso a dicha interfaz mediante un cable conectado al motherboard y accesible desde el exterior, ubicándose el mismo en el compartimiento superior izquierdo la parte inferior del chasis. En la Fig. 11 se observan los bloques de baterías a derecha e izquierda y el cargador de las mismas en el centro. Además del cable a la interfaz JTAG (cable negro con conector blanco compuesto por cables más finos de colores), la Fig. 12 muestra el cable de alimentación eléctrica (de mayor grosor). La conexión con el motherboard se aprecia en la Fig. 13.





La existencia de este cable provoca una situación de riesgo muy elevado, dado que el microcontrolador podría ser reprogramado durante el acto electoral por un usuario malintencionado, teniendo consecuencias imprevisibles. El software del mismo no depende del sistema operativo, y no es posible retornarlo a la versión “de fábrica” mediante un simple reinicio de la máquina. Incluso, sin una auditoría profunda in situ, resulta difícil hasta imposible detectar que el mismo ha sido alterado. Son acciones factibles las siguientes, a modo de ejemplo:

- escritura del chip con datos malintencionados en lugar del voto, no detectable si se emplea una máquina afectada para verificar el voto,
- alteración del texto impreso que puede pasar desapercibido si el votante posee dificultades visuales o no constata visualmente su voto,
- anular el funcionamiento del equipo total o parcialmente,
- alterar el resultado del escrutinio provisorio, mostrando en pantalla el voto impreso pero registrando otro durante el proceso de conteo.

Existe evidencia que este cable se encontró presente durante el proceso electoral del 19 de julio [31] que se replica en la Fig. 14.



C. 3. Detalles del sistema RFID

Respecto del lector RFID, existe la posibilidad de ser anulado (ataque de denegación

de servicio) colocando sobre el mismo una lámina metálica o un chip RFID inválido, que puede estar camuflado con un sticker idéntico al que ya posee o introducirse dentro de la unidad de impresión. Este tipo de ataque a un lector RFID es por demás conocido, como señala Fabienne Serrière para la CanSecWest Applied Security Conference 2008 [32] y si bien es sencillo de revertir en el momento, ocasionaría un gran trastorno, en particular si se realiza a gran escala y demuestra con cuánta facilidad puede anularse el sistema. Y no es posible proteger a la máquina contra él, dado que es inherente al sistema RFID.

Existen múltiples ataques contra el sistema RFID que ya ha sido probado vulnerable incontables veces [33], incluso es posible leer los chips a distancia con el hardware apropiado – simple y de bajo costo [34], [35] – o directamente impedir su funcionamiento [36], y que no debería utilizarse en un proceso electoral [37]. Respecto de la lectura remota, cabe mencionar que la norma ISO 15693 que rige los chips de BUE (ver punto IV. B), establece una distancia de lectura nominal de 70 cm, y una distancia máxima de 1,5 m [38].

D. Otras vulnerabilidades del sistema

En el punto III. D se mencionó que el conteo de votos se realiza al término del horario electoral empleando las máquinas a tal fin. De emplearse una máquina alterada por un usuario malintencionado, el resultado del escrutinio provisorio se vería afectado. Fisanotti menciona que el proceso de transmisión es realizado por otra máquina, no las mismas que las empleadas para emitir sufragio [13]. La patente presentada [39] no abunda al respecto, por lo que no podemos aseverar respecto de esta instancia del proceso.

El servidor central, nomenclado como S-DCS [39], resulta otro punto oscuro del sistema sobre el cuál no poseemos más información.

Tras el análisis de sistema y de las múltiples vulnerabilidades que presenta, hemos encontrado una que denominamos multivoto y que consiste en alterar el contenido del chip RFID con el objeto de emitir más de un voto en una sola boleta. La simpleza de esta vulnerabilidad pone en evidencia la falta de profesionalidad respecto de las reglas del arte con que cuenta todo el sistema Vot.Ar. Referirse al Apéndice B para mayor abundamiento.

V. CASOS DE FRACASO INTERNACIONAL

Distintas aproximaciones a sistemas de voto electrónico han sido abarcadas en el

mundo, muchas de ellas sentando antecedentes de fracaso para sistemas del estilo. Es parte de nuestro objetivo demostrar lo mismo para nuestro país.

A. Israel

Oren y Wool del Laboratorio de Computación y Seguridad de Redes de la Escuela de Ingeniería de la Universidad de Tel-Aviv, Israel, demostraron distintos ataques al dispositivo RFID empleado por el sistema de votación Israelí que permitían leer los votos a distancia, suprimirlos o modificarlos, entre otras cosas [37]. En el caso israelí, los chips RFID eran del tipo ISO 14443 mientras que los chips empleados por MSA son ISO 15693. Si bien existen diferencias entre estos, los principios de funcionamiento son similares [40].

B. Países Bajos

Países Bajos anuló el sistema de votación electrónica a finales del año 2007, por encontrarse graves fallos en el sistema y los procedimientos [41] que permitían a un usuario malintencionado tomar control del sistema [42], del mismo orden que lo mencionado en el presente informe.

C. Alemania

En Alemania, el sistema de votación electrónica fue anulado en el año 2005 al declararse inconstitucional, toda vez que la Constitución alemana establece que cualquier votante debe ser capaz de examinar fidedignamente por completo el proceso de sufragio sin necesidad de conocimiento especializado o técnico, que resulta imposible al incorporarse elementos electrónicos al proceso [43] y [44].

D. EE. UU.

Se emplearon distintos sistemas de voto electrónico en las elecciones del año 2008 en EEUU con el objeto de abaratar los costos del proceso electoral. Sin embargo, un grupo del estado de Maryland (SaveOurVotes) realizó un análisis económico y determinó que el costo del proceso electoral se vió incrementado en aproximadamente 179% por votante [45].

Asimismo, debido a vulnerabilidades en los sistemas de voto electrónico, estos se encuentran en pleno declive desde el año 2012 respecto del uso e implementación, mientras que permanecieron en alza durante el período 1980 – 2012 [46]. “Está ampliamente reconocido que las clásicas boletas de papel son una forma más asequible, fiable y segura para llevar a cabo las elecciones. El voto informatizado es

visto cada vez más como una moda que ha desgastado su acogida.”, concluye Timothy B. Lee luego de exponer algunos casos de fracasos para sistemas de voto electrónico en EE. UU. [47].

VI. SOBRE LA BOLETA ÚNICA DE PAPEL

El sistema de boleta única de papel, también llamado boleta única a secas – implementada en Santa Fe en el año 2010 [48] – o boleta única de sufragio (BUS) [49] – implementada en Córdoba desde el año 2011 -, es una solución simple y efectiva a la problemática que presenta el sistema de boleta partidaria:

- robo de boletas;
- impresión costosa;
- sufragio y escrutinio dificultoso cuando se trata de muchas categorías o muchos candidatos.

La boleta única se trata de un sistema electoral ya probado y efectivo. Tanto en Europa como en América Latina se encuentra en uso este sistema; únicamente en España, Francia y Suecia, en Europa, y Argentina, Uruguay y Brasil, en América Latina, no lo usan de manera extendida o no lo usan en absoluto [50].

Como indicó el vocal de la Junta Electoral Municipal de Córdoba, Leonardo González Zamar, respecto de la implementación de la BUS [51]:

> es indudable que la BUS desalienta o impide viejas prácticas que antes se advertían, como el faltante de boletas de un determinado partido o alianza en el cuarto de votación, cosa que ahora es imposible que suceda.

Por otra parte, como destaca el Dr. Alejandro Groppo, Decano Facultad de Ciencia Política y RR.II. de la Universidad Católica de Córdoba en la presentación del libro *Boleta única: Estudio comparado de los casos de Córdoba y Santa Fe* [52]:

> La boleta única ha demostrado ser un instrumento eficiente, claro y sencillo a los ojos de los ciudadanos, pero por sobre todas las cosas, transparente. La prueba ha sido superada y los resultados son evidentes. Sin embargo, la boleta única no soluciona todos los problemas del sistema político y electoral y por ello no creemos oportuno reclamarle a la misma por los problemas que no está habilitada a solucionar.

Son amplias las ventajas que presenta el sistema de boleta única respecto del sistema de boleta partidaria. Sin embargo, las ventajas del sistema de boleta única electrónica respecto del sistema de boleta única de papel, de existir, no justifican el impacto económico de su alto costo y por sobre todo, la introducción de voto

electrónico en el sistema electoral cuya problemática se ha tratado en el presente.

VII. CONCLUSIONES

Se ha indagado respecto del funcionamiento del sistema *Vot.Ar* / *BUE* de voto electrónico, analizando las distintas partes que lo componen, tanto de manera individual como en conjunto, y en vista de lo presentado se concluye que:

- el sistema presenta vulnerabilidades inherentes a su diseño, que si bien pueden ser salvadas mediante un conteo y revisión manual de votos, este hecho simplemente anula el propósito de tener un sistema de voto electrónico;
- de no realizarse conteo/escrutinio/verificación manual, el resultado del sufragio queda vulnerable al fraude electoral;
- el sistema es oscuro: el código fuente del software es cerrado, así como el hardware y firmware empleado, suprimiendo la libertad de auditar públicamente el sistema y comprenderlo en detalle;
- la forma y el estilo de la programación del sistema no parece realizada bajo los estrictos estándares que requieren aplicaciones de infraestructura crítica;
- no presenta ventajas significativas respecto del sistema de boleta única de papel.

Desde el campo de la seguridad de los sistemas de información evaluamos que **los riesgos que introduce el voto electrónico** en términos de errores accidentales o ataques maliciosos a gran escala y fáciles de encubrir **superan con holgura los beneficios reales o percibidos de la automatización de un paso crítico del sistema electoral**.

Se ha generalizado la creencia que todo sistema social puede ser migrado a un sistema de computadoras, y que esto implica automáticamente una mejora en términos de agilidad y economía, sin ninguna contrapartida. Existen ciertas aplicaciones, con requerimientos críticos de seguridad informática, privacidad y usabilidad, para los cuales la tecnología actual aún no puede dar respuesta. Estos sistemas son complejos y a mayor complejidad, mayor es el riesgo de falla.

La comunidad académica y la industria aún no saben cómo hacer máquinas y sistemas seguros de este tipo. Por esta razón, la buena intención de explorar la migración tecnológica del sistema de votación debe estar englobada en un proyecto que incluya múltiples iteraciones de análisis y retroalimentación con los diversos actores de la comunidad. **Ningún avance técnico debe debilitar la democracia**.

Por todo lo expuesto, consideramos que el sistema no cumple con los objetivos prometidos de brindar seguridad y transparencia y ocasiona un costo adicional al Estado, Ciudad o Municipio que lo emplea.

RECONOCIMIENTOS

A los miembros de CaFeLUG (Sergio Aranda Peralta, Ximena García, Lucas Lakousky, Juan Muguerza, Sergio Orbe, Andrés Paul), a Vía Libre y a nuestros amigos que nos brindan su ayuda aportando opiniones y correcciones.

APÉNDICE A. DETALLES DEL SISTEMA OPERATIVO

Dada la longitud de la respuesta de los siguientes comandos informativos, las publicamos por separado en formato texto legible a excepción de A.3 que es un archivo binario.

- A.1. :~# cat /var/log/dmesg [53]
- A.2. :~# dmidecode [54]
- A.3. :~# dmidecode –dump-bin [55]
- A.4. :~# lsb_release -a [56]
- A.5. :~# lsmod [57]
- A.6. :~# lspci [58]
- A.7. ~# lsusb [59]
- A.8. :~# mount [60]
- A.9. :~# ps aux [61]
- A.10. :~# cat ubnfilel.txt [62]
- A.11. :~# cat ubnpathl.txt [63]
- A.12. :~# uname -a [64]

APÉNDICE B. ATAQUE MULTIVOTO

Hemos publicado previo a las elecciones del 5 de julio la información relevante de este ataque con el objeto de prevenir tanto a los electores como a las autoridades [65], junto a un video explicativo y demostrativo del proceso para mayor ilustración [66].

A. Descripción e impacto del Ataque Multivoto

Al finalizar los comicios, el presidente de mesa abre la urna y comienza el conteo de los votos empleando la misma máquina vot.ar mediante otra función del programa. Para efectuar el conteo:

- Apoya la boleta en la máquina -> se contabiliza un voto.
- Apoya la próxima boleta -> se contabiliza otro voto.

Y así hasta finalizar el recuento. El software de la máquina de voto no permite restar votos al recuento sin volver a cero.

Este proceso no está correctamente implementado, y a través de un error de programación es posible grabar el chip mediante un simple smartphone de forma que contenga múltiples votos a un mismo candidato. Cuando el presidente apoye la boleta en la máquina, ocurrirá lo siguiente:

- Una boleta con chip -> se contabilizan múltiples votos.

B. Detalles técnicos

El pseudo-código del programa que lee y cuenta los votos es:

```
class Selection(object):
 ...
def from_string(TAGcontent):
 datatag = parse(TAGcontent)
...
candidates = []
 for e in datatag.vote:
 party_code = e["party"]
 category_code = e["category"]
 candidate = CandidateClass.get(category_code,
 party_code)
 candidates.append(candidate)
```

Primero se leen los datos del chip de la boleta y se almacenan en la variable datatag. Después se interpreta la selección y se agrega a la lista candidatos. El código no verifica si hay más de un voto para el mismo candidato por elector, y tampoco limita un número máximo de votos por boleta. La función parse() falla también en verificar los datos de forma alguna.

Luego, la clase Count() suma los votos. Este es el pseudo-código:

```
class Count(object):
...
 def add_selection(self, selection, RFIDserial=None):
 if not RFIDserial or not self.serial_exists(RFIDserial):
```

```
for candidate in selection.candidates:
self.results[candidate.party_code, candidate.category_code] += 1
if RFIDserial:
self._RFIDserials.append(RFIDserial)
...
else:
raise RepeatedSerial()
```

Aquí la lista que contiene los múltiples votos es agregada a la variable results. Nuevamente, no hay mecanismo alguno que detecte votos repetidos. La Fig. 15 muestra el resultado del ataque multivoto, donde no coincide la cantidad de votos emitidos con el total de votos contados.

C. Prueba de concepto

Las boletas RFID tienen una estructura simple (referirse al punto IV. B. 1.). Por ejemplo, la siguiente es una boleta para “Diputado” (DIP) “Jefe de Gobierno” (JEF) y “Jefe Comunal” (COM) para la provincia “Buenos Aires” (CABA):

"06CABA.1COM567DIP432JEF123"

Y la siguiente es una boleta que emite tres votos para la categoría “Jefe de Gobierno”:

"06CABA.1JEF123JEF123JEF123"

Y esta es una boleta que emite 10 votos para “Jefe de Gobierno”:

"06CABA.1JEF123JEF123JEF123JEF123JEF123JEF123JEF123JEF123JEF123JEF123"

Hay más posibilidades, por ejemplo, la siguiente boleta emite tres votos normales y luego agrega 7 votos más para “Jefe de Gobierno”:

"06CABA.1COM567DIP432JEF123JEF123JEF123JEF123JEF123JEF123JEF123JEF123"

Los códigos de cada candidato que participa de las elecciones se encuentran publicados en la web [67] y [68], por lo que cualquier persona puede generar los valores correspondientes a fin de emitir un voto malicioso.

Por ejemplo, los códigos para el Ballotage del 19 de julio son (en el orden que se proveen por la web):

- Martín Losteau: 1
- Fernando Sánchez: 4
- Horacio Rodríguez Larreta: 2
- Diego César Santilli: 3
- Voto en blanco: _BLC

Entonces, un multivoto en blanco sería:

```
"JEF_BLCJEF_BLCJEF_BLC"
```

D. Generador de boleta multi-voto

El siguiente script en Python genera el CRC32 en little-endian sobre los datos indicados, a fin de escribirlos en el chip. Se pueden introducir estos valores manualmente en una aplicación de escritura NFC para Android como NFC-V [69].

```
from zlib import crc32
from struct import pack
voto="06CABA.1COM1234DIP5678JEF5678" # original
voto="06CABA.1COM1234JEF5678JEF5678" # 2 JEF
print "Largo del mensaje: %02X" % len(voto)
print "CRC: %s" % ' '.join(map(lambda x:"%02X"%ord(x),pack("i",crc32(voto))))
print "Datos de boleta: %s" % ' '.join(map(lambda x:"%02X"%ord(x),voto))
```

E. Solución paliativa

La solución de fondo de este problema es no emplear sistemas de emisión del sufragio por medios informáticos. Estos agregan nuevas posibilidades de ataques y fraudes sin solucionar ninguno de los problemas característicos de nuestro sistema electoral que no pueda ser resuelto con la boleta única de papel. **El sistema Vot.Ar fue impuesto de forma apresurada**, sin educación apropiada a los ciudadanos ni las autoridades y sin una auditoría de código exhaustiva, como claramente deja en evidencia este ejemplo de error de programación. Por otra parte, la experiencia internacional muestra que todo sistema de voto electrónico, más temprano que tarde, ha resultado vulnerable a alguna forma de ataque. Situaciones todas que han sido tratadas en el presente informe.

Como paliativo al ataque mostrado, recomendamos enfáticamente a los presidentes de mesa y a los fiscales realizar la contabilidad boleta por boleta haciendo énfasis en la impresión por sobre la información del chip. Es indispensable asegurarse de que la cantidad de boletas coincide exactamente con los votos contados por la

máquina. Aconsejamos desarrollar un procedimiento manual en paralelo, ejecutado por las autoridades de mesa y los fiscales del mismo modo que históricamente se ha ejecutado para las elecciones convencionales.

REFERENCIAS

[1] Lozano,Tribunal Superior de Justicia de CABA, Resolución Nº 127/15. Disponible en: https://www.eleccionesciudad.gob.ar/uploads/resoluciones/resoluci%C3%B3n%20127.pdf

[2] En la última versión vista (>=3.0) se ha activado el bloqueo de escritura del chip, impidiendo la reescritura del mismo. Esto es, si el chip fue grabado mediante la máquina de votar (en modo votación), el mismo no puede volver a grabarse.

[3] Es necesario realizar un análisis químico sobre el papel a los efectos de determinar la vida útil de la BUE.

[4] Honorable Senado de la Nación Argentina, Constitución Nacional, Capítulo II: Nuevos Derechos y Garantías. Disponible en: http://www.senado.gov.ar/Constitucion/capitulo2

[5] Página web de Vot.Ar: http://www.vot-ar.com.ar/#sobre

[6] ¿Qué es el Software Libre?. Disponible en: https://www.gnu.org/philosophy/free-sw.es.html

[7] Hardware de Fuentes Abiertas. Disponible en: http://www.oshwa.org/definition/spanish

[8] Tribunal Superior de Justicia de la Ciudad Autónoma de Buenos Aires, Simulador BUE. Disponible en: https://www.eleccionesciudad.gob.ar/simulador/#

[9] Gobierno de la Ciudad de Buenos Aires, Centros de Consulta de BUE. Disponible en: http://www.buenosaires.gob.ar/boletaelectronica

[10] Centro de Documentación Municipal, Dirección General de Información y Archivo Legislativo, ANEXO de la LEY Nº 4.894. Disponible en: http://www.cedom.gov.ar/es/legislacion/normas/leyes/anexos/al4894.html

[11] Vídeo demostración de inicialización del sistema y sufragio. Disponible en: https://youtu.be/Riee68LCRA0

[12] Las boletas que no hayan podido ser leídas por el lector RFID son consideradas

“voto no leído por razones técnicas”, se almacenan en un sobre y se envían al Tribunal a los efectos de ser procesados manualmente durante el escrutinio definitivo.

[13] Juan Pedro Fisanotti, FisaDev, Voto electrónico con Python y Ubuntu. Disponible en: http://fisadev.blogspot.com.ar/2011/04/voto-electronico-con-python-y-ubuntu.html

[14] Vot.Ar Versión >=3.0. Se ejecuta la funcion md5_checkfiles() definida en la línea 113 del archivo app/msa/voto/modulos/administrador.py

[15] Claudio Enrique Righetti, FCEyN UBA, OAT Nº 03/15 – Auditoría de sistemas Elecciones 2015 – Ciudad de Buenos Aires. Disponible en: https://www.eleccionesciudad.gob.ar/uploads/OAT%20n%203-15-06012015204749.pdf

[16] Tribunal Superior de Justicia, Ciudad Autónoma de Buenos Aires, Ley 4894: Régimen normativo de Elecciones Primarias, Abiertas, Simultáneas y Obligatorias y de Boleta Única y Tecnologías Electrónicas de la Ciudad. Disponible en: http://tsjbaires.gob.ar/index.php?id=3899&cid=5202&fid=16&task=download&option=com_flexicontent&Itemid=49

[17] Claudio Enrique Righetti, FCEyN UBA, OAT Nº 03/15 – Auditoría de sistemas Elecciones 2015 – Ciudad de Buenos Aires. Página 9, Párrafo 1.

[18] Claudio Enrique Righetti, FCEyN UBA, OAT Nº 03/15 – Auditoría de sistemas Elecciones 2015 – Ciudad de Buenos Aires. Página 9, Párrafo 9.

[19] Claudio Enrique Righetti, FCEyN UBA, OAT Nº 03/15 – Auditoría de sistemas Elecciones 2015 – Ciudad de Buenos Aires. Página 10, Párrafo 3.

[20] Claudio Enrique Righetti, FCEyN UBA, Anexo II, OAT Nº 03/15 – Auditoría de sistemas Elecciones 2015 – Ciudad de Buenos Aires. Página 16, Párrafo 4

[21] Departamento de Informática, ITBA, DVT 56-504: Auditoría de Sistema de Votación Electrónica 2015 para la Defensoría del Pueblo de la C.A.B.A. Disponible en: http://defensoria.org.ar/wpnoticias/wp-content/uploads/2015/06/InformeAudotoriaVotoElectronico.pdf

[22] Departamento de Informática, ITBA, DVT 56-504: Auditoría de Sistema de Votación Electrónica 2015 para la Defensoría del Pueblo de la C.A.B.A. Página 1, Párrafo 3.

[23] Departamento de Informática, ITBA, DVT 56-504: Auditoría de Sistema de Votación Electrónica 2015 para la Defensoría del Pueblo de la C.A.B.A. Página 6, Sección 3, Recomendación 1.

[24] Departamento de Informática, ITBA, DVT 56-504: Auditoría de Sistema de Votación Electrónica 2015 para la Defensoría del Pueblo de la C.A.B.A. Página 9, Recomendación 9.

[25] NXP, I-CODE SLI Smart Label IC SL2 ICS20, Datasheet. Disponible en: http://www.nxp.com/documents/data_sheet/SL058030.pdf

[26] NXP, I-CODE SLI Smart Label IC SL2 ICS20, Datasheet. Sección 3.2.5, Página 10.

[27] SAM7X256 member of the Atmel SAM7X series of microcontrollers, ATMEL. Disponible en: http://www.atmel.com/devices/SAM7X256.aspx

[28] Security Reseach Labs, Turning USB peripherals into BadUSB. Disponible en: https://srlabs.de/badusb

[29] Vot.Ar Versión >=3.0. Constante SERIAL_PORT, línea 2 del archivo app/msa/core/armve/settings.py

[30] SAM7X512 / SAM7X256 / SAM7X128 Datasheet, ATMEL. Página 2, ítem 2, subítem 2. Disponible en: http://www.atmel.com/Images/Atmel_32-bit-ARM7TDMI-Flash-Microcontroller_SAM7X512-256-128_Datasheet.pdf

[31] Javier Smaldone, El sistema oculto en las máquinas de Vot.Ar. Disponible en: https://blog.smaldone.com.ar/2015/07/15/el-sistema-oculto-en-las-maquinas-de-vot-ar

[32] Fabienne Serrière, 2008, RFID reader denial of service. Disponible en: http://hackaday.com/2008/06/09/rfid-reader-denial-of-service

[33] Veo Zhang, TrendLabs, 2014, Hacking RFID Payment Cards Made Possible with Android App. Disponible en: http://blog.trendmicro.com/trendlabs-security-intelligence/hacking-rfid-payment-cards-made-possible-with-android-app

[34] Joseph Gates,Vishwajeet Potnis, Matthew Howell, William Tran, Louisiana State University, Baton Rouge, Louisiana, Using ISO 15693 Compliant RFID Tags in an

Inventory Control System. Disponible en: http://www.ieee.org/education_careers/education/standards/using_iso_15693_compliant_rfid_tags.pdf

[35] Sean Michael Kerner, 2013, Hacking RFID Tags Is Easier Than You Think: Black Hat. Disponible en: http://www.eweek.com/security/hacking-rfid-tags-is-easier-than-you-think-black-hat

[36] Tom Espiner, ZDNet, 2006, RFID DoS attacks ‘proven’. Disponible en: http://www.zdnet.com/article/rfid-dos-attacks-proven

[37] Yossef Oren y Avishai Wool, Computer and Network Security Lab School of Electrical Engineering, Tel-Aviv University, Ramat Aviv 69978, Israel, 2010, RFID-Based Electronic Voting: What Could Possibly Go Wrong?. Disponible en: http://www.eng.tau.ac.il/~yash/evoting-relay-rfid2010.pdf

[38] ISO/IEC 15693-1:2010. Disponible en http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=39694

[39] MSA Magic Software Argentina, Memoria Descriptiva de la patente de invención sobre Disposición y Método de Voto Electrónico. Disponible en: http://www.vialibre.org.ar/wp-content/uploads/2015/05/memoria.descriptiva.patente.votoelectronico.pdf

[40] John Wehr, SecureIDNews, 2003, Contactless card standards: Making sense of 10536, 14443, and 15693. Disponible en: http://www.secureidnews.com/news-item/contactless-card-standards-making-sense-of-10536-14443-and-15693/

[41] Jan Libbenga, The Register, 2007, Dutch pull the plug on e-voting. Disponible en: http://www.theregister.co.uk/2007/10/01/dutch_pull_plug_on_evoting

[42] Rop Gonggrijp, Willem-Jan Hengeveld et al., Stichting “Wij vertrouwen stemcomputers niet”, 2006, Nedap/Groenendaal ES3B voting computer: a security analysis. Disponible en: http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf

[43] National Democratic Institute, The Constitutionality of Electronic Voting in Germany. Disponible en: https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany

[44] Judges Voßkuhle, Broß, Osterloh, Di Fabio, Mellinghoff, Lübbe-Wolff, Gerhardt, Landau, Bundesverfassungsgericht, 2009, Judgment of the Second Senate of 3 March

2009 on the basis of the oral hearing of 28 October 2008 – 2 BvC 3/07, 2 BvC 4/07 –. Disponible en: http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/03/cs20090303_2bvc000307.html

[45] Kiim Zetter, Wired, 2008, The cost of e-voting. Disponible en: http://www.wired.com/2008/04/the-cost-of-e-v

[46] ProCon, 2013, Voting Systems & Use: 1980-2012. Disponible en: http://votingmachines.procon.org/view.resource.php?resourceID=000274

[47] Timothy B. Lee, ars technica, 2012, Paper prophets: Why e-voting is on the decline in the United States. Disponible en: http://arstechnica.com/features/2012/10/paper-prophets-why-e-voting-is-on-the-decline-in-the-united-states

[48] Ley 13.156: Sistema de Boleta Única y Unificación del Padrón Electoral, Santa Fe, 7 de febrero de 2011.

[49] Juzgado Electoral De La Provincia De Cordoba, Ley Nº 9571: Código Electoral Provincial. Disponible en: http://www.justiciacordoba.gob.ar/jel/pdf/capacitacion/CompendioLegislacionElectoral.pdf

[50] Matías Bianchi[et al.]; con colaboración de Mario Navarro [et al.], Boleta única: Estudio comparado de los casos de Córdoba y Santa Fe, UNR Editora, Rosario, 1ra edición, 2013.
Página 17. Disponible en: http://www.asuntosdelsur.org/sitio2013/wp-content/uploads/downloads/2013/11/Libro-Boleta-Unica.pdf

[51] Telam, 18 de Septiembre de 2011, Jueces destacan el valor de la boleta unica de sufragio, Córdoba. Disponible en: https://es-us.noticias.yahoo.com/jueces-destacan-valor-boleta-unica-sufragio-171601564.html

[52] Matías Bianchi[et al.]; con colaboración de Mario Navarro [et al.], Boleta única: Estudio comparado de los casos de Córdoba y Santa Fe, UNR Editora, Rosario, 1ra edición, 2013.
Página 5.

[53] A.1. dmesg.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/dmesg.txt

[54] A. 2. dmidecode.txt. Disponible en: https://github.com/HacKanCuBa/informe-

votar/blob/master/Anexo%20A/dmidecode.txt

[55] A. 3. dmidecode binary dump. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo %20A/dmidecode.bin

[56] A. 4. lsb_release.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/lsbrelease.txt

[57] A. 5. lsmod.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/lsmod.txt

[58] A. 6. lspci.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/lspci.txt

[59] A. 7. lsusb.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/lsusb.txt

[60] A. 8. mount.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/mount.txt

[61] A. 9. report of proceses, ps.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/ps.txt

[62] A. 10. ubnfilel.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/ubnfilel.txt

[63] A. 11. ubnpathl.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/ubnpathl.txt

[64] A. 12. uname.txt. Disponible en: https://github.com/HacKanCuBa/informe-votar/blob/master/Anexo%20A/uname.txt

[65] Francisco Amato, Iván A. Barrera Oro, Enrique Chaparro, Sergio Demian Lerner, Alfredo Ortega, Juliano Rizzo, Fernando Russ, Javier Smaldone, Nicolas Waisman, 3 de julio de 2015, Ataque a sistema de voto electrónico Vot.Ar (BUE) permite sumar multiples votos con una sola boleta. Disponible en: https://docs.google.com/document/d/1aH6kvoLR8O1qWOpEz89FAB2xFcBNB-QqHgZpXxg0vGE/preview

[66] Sumando múltiples votos con una boleta en el sistema vot.ar, video demostrativo. Disponible en: https://www.youtube.com/watch?v=CTOCspLn6Zk

[67] Datos sobre los códigos. Disponible en: https://www.eleccionesciudad.gob.ar/simulador/datos/

[68] Códigos de los candidatos. Disponible en: https://www.eleccionesciudad.gob.ar/simulador/datos/CABA/Candidatos.json

[69] STMicroelectronics, NfcV-reader, Google Play. Disponible en: https://play.google.com/store/apps/details?id=com.nfc.apps&hl=es

[70] NXP, I-CODE SLIX SL2S2002, Datasheet. Disponible en: http://www.nxp.com/documents/data_sheet/SL2S2002_SL2S2102.pdf

---

